Vol. [46], Issue [1], Year (2020)

ANALYZING AND EVALUATING THE SECURITY STANDARDS IN WIRELESS NETWORK: A REVIEW STUDY

Intisar Shadeed Al-Mejibli[1]
[1] *University of Information Technology and Communications, Baghdad, Iraq*
dr.intisar.almejibli@gmail.com

Dr. Nawaf Rasheed Alharbe[2]
[2] *Taibah University, College of Community, Badr, Kingdom of Saudi Arabia*
nawaf_3130@hotmail.com

Abstract **- Wireless networks used widely in office, home, and public places so security is one of the significant issues to keep the transmitted information safe. The applied security standards have been developed in response to the demand of high security and the developed hardware with software. Currently, the available security standards are (WEP, WPA, WPA2 and under development WPA3). These security standards are different in the offered security level base on the employed authentication method and encryption algorithms. The major objective of this paper is studying security standards and analyzing them based on their features. In addition to presenting a detailed review about WPA3 and its improvements over the older security standards. The conducted evaluations explained the differences among the Wi-Fi security standards in term of the offered security level, software and hardware requirements.**

Keywords - Security Standards, Wireless Network, WEP, WPA, WPA2, WPA3.

I. INTRODUCTION

The technology of wireless releases the wire network users from copper wires. With wireless technology, a user can freely move and use devices such as laptop and cell phone. Hence, users can stay online whenever the wireless signal is available. Based on wireless technology principle, electromagnetic waves are used to carry the signals then these waves are transmitted to the receiver of signal. Table 1 categorizing the wireless technology into three layers [1].
Currently the Wireless technologies are employed in everywhere since it featured with the low cost, mobility and simplicity [2]. This rapid growth of this technology requires tackling its limitations in order to seamless its usage. Sending the packet by air makes it vulnerable, so security is needed to prevent eavesdropping by third party. Thus, secreting data during transmitting is very significant to prevent eavesdropping [3]. In addition, many application suggested the use of additional methods to secure the exchanged data [4].

TABLE 1. THE WIRELESS TECHNOLOGY REGARDING THEIR LAYERS

Layer	Technologies
Application and service	Wireless applications: WAP, i-mode, messaging, Voice over Wireless network, etc.
Physical	Wireless standards: 802.11a, 802.11b, 802.11g, WLAN 802.11i etc.
Device	Mobile devices: Notebooks, cellular phones, wearable computers, etc.

There are two concepts of security, which are authentication and encryption. Authentication is a process by which the user identification is assured depend on predefined credentials such as passwords or specified digital certificates [5]. Encryption process targets the traffic passing the wireless network so it scrambles the data unreadable while passing the air. There many techniques that have been used to accomplish the encryption such as Rivest Cipher 4 (RC4) [6], Temporal Key Integrity Protocol (TKIP), and Advanced Encryption Standard (AES) [6] with Cipher Block Chaining Message Authentication Code Protocol (CCMP) [5, 8].

This paper examine the security standards in wireless networks including WEP, WPA, WPA2 and WPA3.

The remaining of this paper is arranged as following: Section 2 describes wireless Security history. Related work is summarized in section 3. Section 4 describes wireless security issues. Section 5 presents wireless security requirements. Wireless security standards are detailed in section 6. Analyzing and evaluation are showed in section 7. Section 8 explains the WPA3 improvements. The conclusion is presented in section 9.

II. WIRELESS SECURITY HISTORY

In 1997, the 802.11 Wireless LAN standard is explained by the Institute of Electrical and Electronic Engineers (IEEE) [9]. Many wireless security standards were developed to be employed in wireless networks at homes, offices and public area. The used wireless security protocols are WEP, WPA, and WPA2, where each of them has its own strengths and weaknesses. In addition to, upcoming standard WPA3 which is expected to be used in the late of 2019. Figure 1 shows the

history of each security standard. These four major generations of security standards are explained in the following:

WEP (Wired Equivalent Privacy)
WPA (Wi-Fi Protected Access)
WPA2/802.11a,b,g (Wi-Fi Protection Access, Version 2)
WPA3/802.11i (Wi-Fi Protection Access, Version 3)

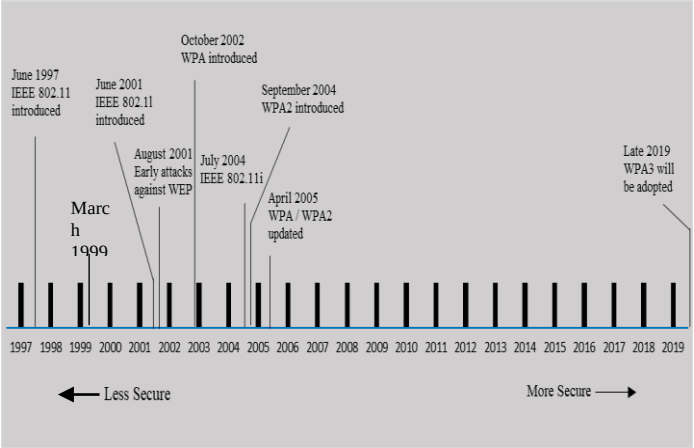

Fig. 1. Wi-Fi Security Standards

III. Related Work

There is a lot of effort that have been made in field studying wireless security standards with their software and hardware requirements. The following presents some researches that have been accomplished in this area:

Authors in [10] presented an overview of the security standards WEP, WPA and WPA2. In particular, they discussed in detail the procedure of cracking WEP and WPA2. The concluded results show that the proper setup of any wireless could prevent it from being exposed to successful hacking attempts.

In [11] the authors presented a comparison among WEP, WPA and WPA2. They modulate the scripts of legendary attack vector, which is Air crack, set of tools in order to examine the authentication of all three standards. They used Back Track operating system in test operation. The result showed that WEP is the weakest and WPA was a temporary solution. From other hand, WPA2 outperforms the other protocols, as it is very solid and long-term solution.

The authors in [12] presented a survey about the different security standards. In particular. This study focused on understanding the principles of security standards in wireless network and specifying the advantages and disadvantages of these standards.

In [13] the authors focused on highlighting the vulnerabilities of WPA2/WEP/WPA2-PSK and suggesting solutions for them. This research studied the evolution of the available security techniques and presented a comparison among them. The

results shows that WPA2 is the most recommended techniques for wireless networks. Additionally, it proposed to use another encryption technique to tackle the WP2 shortcomings.

Authors in [14] investigated and compared the algorithm WEP, WPA and WPA2. The analyzing of this study were in terms of their implementations along with their possible vulnerabilities.

In [15] the authors presented a comparative study among the applied encryption mechanisms in WEP and WPA to understanding their working concepts and security bugs. In addition, they studied the security protocols abilities in authenticate the users. Further, the research shows how easy it is to crack the security techniques of wireless networks by using the suite of tools named aircrack-ng and commview software, which has ability to assess WiFi network security.

Authors in [16] have been presented wireless security standards WEP, WPA and WPA2. This research investigated the improvements of WPA2 over WEP and WAP standards. From other hand, it presented the vulnerabilities of WPA2. This research concluded some suggestions to enhance the security of wireless network.

In [17] the authors presented a survey of WEP, WPA and WPA2 that explains all their features including their weaknesses and improvements. In addition to, presenting a comparative study among WEP and WPA and WPA2.

All the aforementioned researches studied WEP, WPA, and WPA2. While this paper studies these wireless network security standards in addition to WPA3.

IV. Wireless Security Issues

Wi-Fi is a technology offers wireless local area networking within a range of approximately 46 meters indoors and 92 meters outdoors based on used access point. All the devices covered by the service of access point can access data that is sent to or from the access point. Although, this feature provides easily access to wireless network, it opens the door for security threads. The security is much more important and mandatory in wireless networks than wired networks. This is attributed to broadcasting the information in wireless network for the neighborhoods to hear. Using wireless network to send critical information by financial institutions, banks, military networks or information concerning to terrorists etc. requires taking extra measures for protection [18, 19].

The attacks on wireless network may be categorized into two main classes' passive attacks and active attacks according the interruption of communication act. Figure 2 shows the attacks on wireless networks.

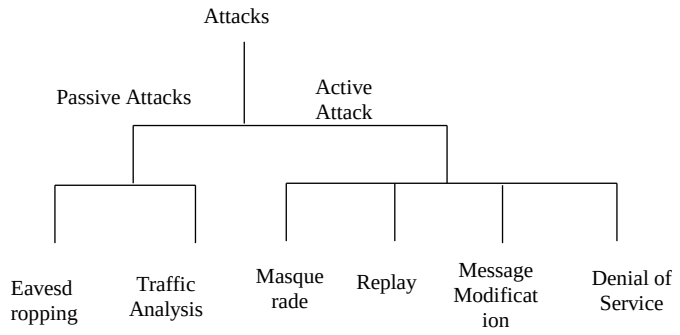

Fig. 2. The Types of Attacks on Wireless Network

Passive attack obtains information that being transmitted in the network without disturbing the communication. Whereas active attack disrupts the normal network functionality, implies it may interrupt the communication, modify or fabricate information [20, 21, 22].

- **Passive attacks**: Passive attacks eavesdrop or spoof on information where the attacker attempts accessing the being transmitted data illegally. Passive attacks may be categorized into two kinds:
  - **Eavesdropping**: In such kind of attacks, the attacker attempts access the messages of email or the being transferred file.
  - **Traffic analysis**: In this kind of attack, the attacker tries disclose the location and identity of connected nodes. In addition, the attacker can observe the length and frequency of messages that being transmitted where these information are useful in guessing to specify the nature of the being transmitted information.
- **Active attacks**: these attacks has four subclasses as following:
  - **Masquerade:** in this kind of attacks, an entity pretends to be to be an authorized entity to gain access to special information or to gain greater privileges.
  - **Reply:** In this kind of attacks, the data is captured passively and then they maliciously or fraudulently repeated or delayed.
  - **Modification:** In such kind of attacks, the hacker tries exchange the messages or delaye them.
  - **Denial of Service:** In which the attacker prohibits legitimate users from accessing specific services or other IT resources.

V. Wireless Security Requirements

There are four characteristics that must be taken into consideration in developing an ideal security system. These characteristics are [19, 21]:

- **Authenticity:** Authenticity indicates identifying the authorized users from unauthorized users. This can be performed by verification the node identity in network. Any connected nodes in wireless networks must first verify their identities to each other [19].
- **Confidentiality:** The confidentiality implies limiting the wireless network access to authorized users only and blocking the unauthorized users from accessing the wireless network and disclosure the information. The type of access is based on the user privilege for instance read only, printing, or knowing the object is permitted [19].
- **Integrity:** The integrity refers to maintain the information accuracy and reliability when transmitting it through wireless network. Therefore, the information must be never changed while. Only the authorized users are able to perform modification operation on transmitted information such as substitution, insertion or deletion of data.
- **Availability:** This characteristic implies that wireless network is indeed available to the authorized users for accessing upon their request. Denial of service is contrary of availability, which result in blocking the authorized users from accessing the wireless network. Hence, the user will be unsatisfied [19, 21].

VI. Wireless Security Standards

This section details the Wi-Fi Security standards includes WEP, WPA, WPA2 and WPA3. All the features of the investigated wireless security standards are presented as following:

A. Wired Equivalent Privacy WEP

WEP was introduced in the first IEEE 802.11 standard back in 1999. Figure 3 shows the WEP encryption scheme where CRC-32 is Cycle Redundancy Check.

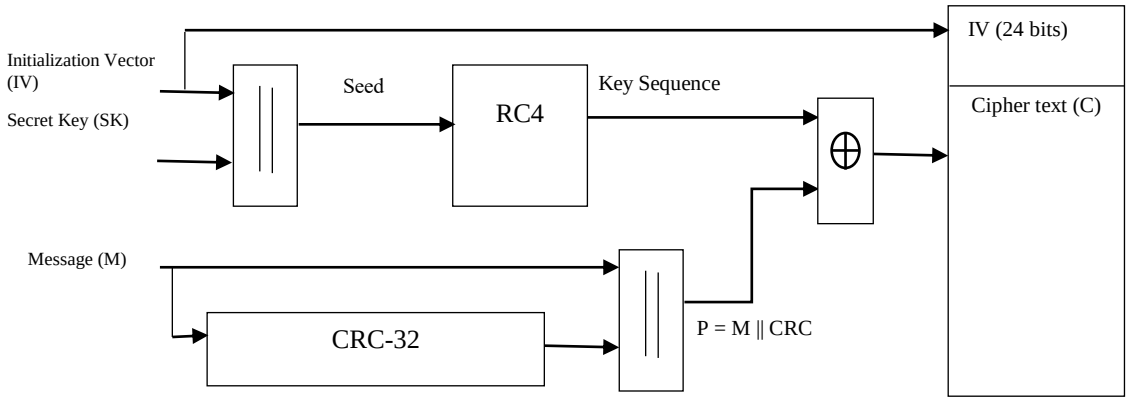

Fig. 3. WEP Encryption Scheme

It based on the Rivest Cipher 4 (RC4) security algorithm, which offers the security to sent data over wired LAN by encryption/ decryption data in sender and receiver sides. The final encrypted message is composed from adding the IV at the beginning of the Cipher text.

In 2003, a free available software can cracked the passwords of WEP in minutes. In 2004, the Wi-Fi Alliance officially abandoned WEP standard [23, 24].

B. Wi-Fi Protected Access (WPA)

WPA is a specification of data encryption introduced by the Wi-Fi Alliance for 802.11 Wireless Networks that tackles the weaknesses of WEP without the need of changing the hardware.

WPA enhance WEP by using dynamic encryption keys instead of static encryption key to provide more security to network [25]. Figure 4 shows the WPA encryption scheme.

WPA based on RC4 and Temporal Key Integrity Protocol (TKIP). It extended the key values and the IV to 128 bits. It was expected to remove the redundant IV deficiency in addition to attacks of stop brute force key.

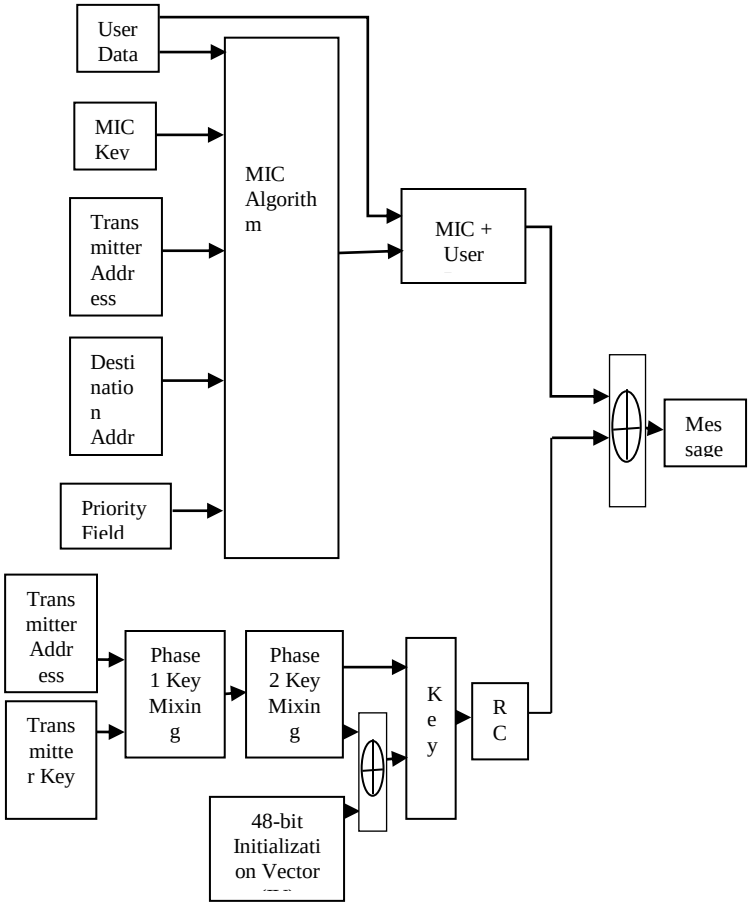

Fig. 4. The WPA Encryption Scheme

In general, the usage of WEP algorithm revealed that it was inefficient. However, it requires modifications more than just expanding the IV and key sizes. As a result, both the WEP2 name and original algorithm were discarded. The two extended key lengths stay in use and then became WPA's TKIP.

TKIP enhances WEP by adding a 128-bit before the key packet depending on a mixing function to overcome the earlier weak of WEP Keys. In addition to, using a re-keying mechanism to strength the keys of encryption and integrity. The two modifications makes TKIP Keys more strength against the hacker attacks [24, 26].

C. Wi-Fi Protected Access version 2 (WPA2)

Currently, Wi-Fi Protected Access II is deployed for wireless security by the most wireless access points with a pre-shared key, and it known as WPA2-PSK.

WPA2 uses the Advanced Encryption Standard (AES), Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) for encryption instead of using CR4 with TKIP as in WPA to improve the security level. If a device cannot support CCMP, WPA2 supports TKIP as well. Currently, it is considered as the best security standard. However, it is has several vulnerabilities. Figure 5 shows the WPA2 encryption scheme.

WPA2 standard produces scalable and robust security architecture by separating the user authentication from the enforcement of message integrity and privacy. This security architecture is suitable to equal prowess networks such as home networks and corporate networks [24].

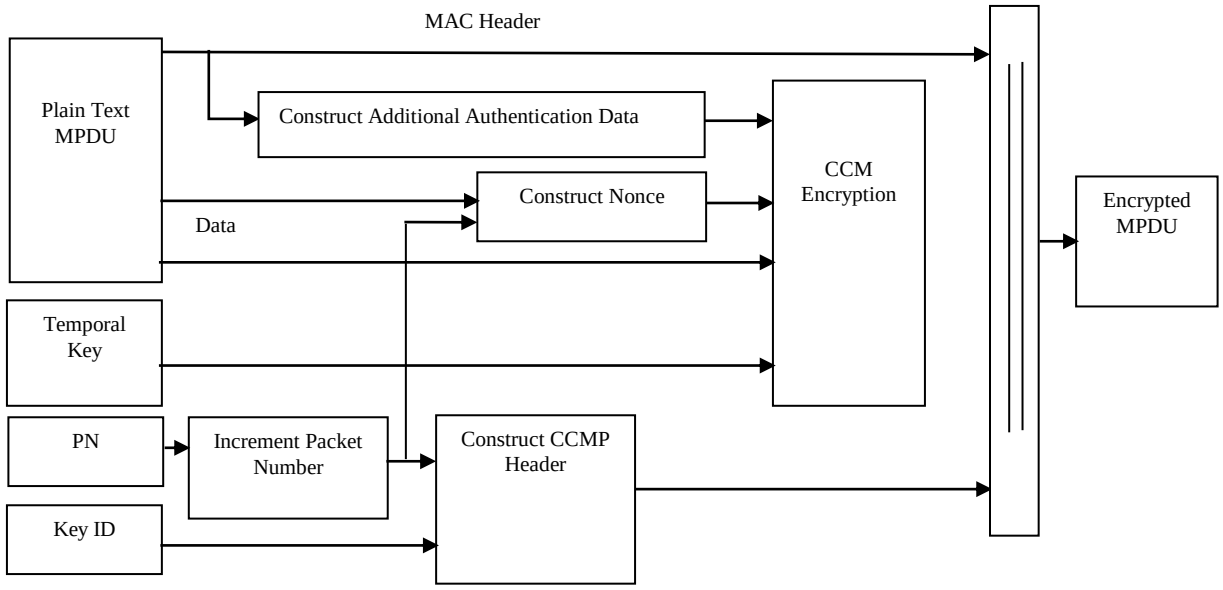

Fig. 5. The WPA2 Encryption Scheme

However, the main weakness of WPA2 mechanism is when the attacker can to access secured network of WiFi and can reach a particular keys to execute an attack on other devices connected to the network. Although, breaking secured network of WPA/WPA2 through this hole needs about 2 to 14 hours, it is still a crucial security issue and must be tackled [23, 24].

D. Wi-Fi Protected Access version 3 (WPA3)

WPA3 is the next upgraded version of Wi-Fi WPA security standard which announced by Wi-Fi alliance at January 2018. WPA3 developed in to two modes Personal and Enterprise. Where the first boost the security of the protocol of secure key establishment by using Simultaneous Authentication of Equals (SAE) to provide robust protection for password authentication and the process of secure configuration is simplified for all devices. The second mode aims to boost security in workplace Wi-Fi networks. Where it improves the strength of cryptographic through applying 192-bit security protocols, which is defined in the Commercial National Security Algorithm (CNSA) Suite. CNSA offers the latest in cryptographic strength to various environments such as government and defense [27, 28, 29, 30]. WPA3 based on the success of WPA2 and aimed to deliver a suite of features that improve device configuration, authentication, encryption, and consistency of security protocols.

In WPA3, these features have been sophisticated to achieve two main benefits.

First: facilitate the Wi-Fi device security for both users and service providers, and second provide personal and enterprise Wi-Fi networks with advanced security [28, 29].

With WPA3, the privacy in open networks is increased by deploying Opportunistic Wireless Encryption (OWE) which delivers each user individual data encryption Wi-Fi Protected Access. [27, 28, 31].

VII. Analyzing and Evaluating

WEP is different form WAP and WPA2 in required hardware and employed software. Although WPA2 based on different hardware from WEP and WAP, it support the employed software by WEP and WPA. Table 2 shows the differences among WEP, WAP, WPA2 and WAP3 in terms of encryption and authentication approaches [32].

In WPA2, 'brute force' attack was probably used to discover the Wi-Fi password. This is attributed to the procedure of predicting password which could happen offline. In WPA3 brute force attacks are successfully avoided because new standard permits prevent hackers from predicting password offline. This is the advantage of using WPA3-SAE instead of using WPA2-PSK. The differences in encryption process among the investigated Wi-Fi security standards are depended on the employed encryption algorithms. Table 3 represents the differences among the employed encryption algorithms.

In general, the following shows the security standards that basically rated from best to worst based on the modern Wi-Fi security methods available on modern (after 2006) routers:

1. WPA2 + AES
2. WPA + AES
3. WPA + TKIP/AES (TKIP is there as a fallback method).
4. WPA + TKIP
5. WEP
6. Open Network (no security at all) [20].

Table 2. The Differences among WEP, WAP and WAP2

	WEP	WPA	WPA2	WPA3
Encryption	RC4	RC4 and TKIP	AES and CCMP	GCMP-256
Authentication	Uses its key as authentication	Can use 802.1x and EAP	Can use 802.1x and EAP	Simultaneous Authentication of Equals (SAE)
Device Compatibility	802.11a,b,g	802.11a,b,g	802.11a,b,g	WLAN 802.11i
Security Level	Weak	Better than WEP	Better than WEP & WPA	Best
Security Speed	Slowest	Midst	Fast	Faster than older
Processing Power	Not much processing power	Needs less processing power than WPA2	Needs more processing power than WPA	Needs more processing power than WPA2
Master Key	Master keys are used directly	Master keys are never directly used	Master keys are never directly used	-
Data Integrity	CRC-32	Message Integrity Code MIC Algorithm.	Cipher block chaining message authentication code (CBC-MAC)	256-bit Broadcast/ Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)
Key Management	None	4-way Handshake	4-way Handshake	384-bit Elliptic Curve Diffie-Hellmen (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA)
Hardware Compatibility	Possible to deploy on current hardware infrastructure	Possible to deploy on both current and previous hardware	Older Network Interface Cards are not supported. Only the 2006 and newer	Possible to deploy on WPA2 hardware with software updates
The Attack with the most Threat	Vulnerable against Chopchop, Bittau's fragmentation and Denial of Service DoS attacks including variety of DoS attacks.	Vulnerable against Chopchop, Ohigashi-Morii, WPA-PSK, and Dos attacks	Vulnerable against DoS attacks due to unprotected control frames and MAC spoofing	Vulnerable against SSL Stripping, Evil Twin Attack and DNS Spoofing

TABLE 3. THE DIFFERENCES AMONG RC4, RC4 WITH TKIP AND AES WITH GCMP

	RC4	RC4 with TKIP	AES with CCMP	GCMP-256
Cipher Mode	Stream	Stream	Block	Block
Key Rotation	None	Dynamic Session Keys	Dynamic Session Keys	Dynamic Session Keys
Key Size	40 - 2,048 (Bits)	80 Bits	192 – 256 bits	256 - Bits
Key Distribution	Manually typed into each device	Automatic distribution available	Automatic distribution available	Automatic distribution available

VIII. . THE WPA3 IMPROVEMENTS

The WPA3 Wi-Fi security provides many improvements that can be summarized as the following:

1- Much harder passwords to be cracked: When WPA2 is employed, an attacker can guess password by using dictionary-based attack, which based on some captured data from intended Wi-Fi stream.
Whereas WPA3 this is not possible because it requires attackers to be online and interact with Wi-Fi for every password guess. Hence WPA3 makes cracking the passwords much harder and time-consuming [27, 28, 29, 31].

2- Much safer for old data: In WPA3, if a cracker can guess password of the saved encrypted data, he/she cannot decrypt that old data. The cracker can only decrypt newly captured data this is because WPA3 supports "forward secrecy". Thus, with WPA 3 the user must change the password as soon as possible [28, 29, 31].

3- Facilitate setting up the smart home devices: WPA3 makes it much easier to setting up the smart home devices with "Wi-Fi Easy Connect". This feature offers the user the ability of connecting a device by merely scanning a QR code on user's phone. Although WPA2 included the feature named "Wi-Fi Protected Setup" which in somewhat similar to "Wi-Fi Easy Connect", it suffer from a number of security vulnerabilities [28, 29, 31].

4- More secure for public Wi-Fi networks: WPA3 encrypts the user individual traffic in public and open Wi-Fi network, to make them much safer to employ. In contrary to the current Wi-Fi standards, which are horribly insecure for open and public Wi-Fi networks. In open and public Wi-Fi network that doesn't require password, it is easy for attackers to sniff out personal information [29, 31].

WPA3 is expected to hit mass adoption in late 2019 this is the Wi-Fi alliance prediction [28, 31, 33].

CONCLUSION

This research presented an analyzing and evaluating study in known wireless security standards, which are WEP, WPA, WPA2 and WPA3. This study investigated these standards based on their features such as employed encryption and authentication methods. In addition to, describing the vulnerable to attacks.
The encryption methods were explained in details based on the employed encryption algorithm. The evaluated results showed that the WPA2 with AES accomplished better level of security than the WEP and WPA however it still vulnerable to some attacks such as Denial of Service (DoS). Thus, security in wireless network requires more attention from researchers to propose robust security standard that has ability to overcome the aforementioned attacks. Currently, WPA3 Wi-Fi security standard is under developing and it aims to overcome the older security standards vulnerabilities and offer high level of security. The routers that able to implement WPA3 are already being marketed, but they need to be update with new software, which the manufacturers are working on. So that the users can implement WPA3 in their devices.

REFERENCES

1. Chris Weber and Gary Bahadur. November 2009. Wireless Networking Security. Microsoft TechNet. https://technet.microsoft.com/en-us/library/bb457019.aspx
2. Nidal Aboudagga, Damien Giry and Jean-Jacques Quisquater. May 2014. Wireless Security Design Overview. file:///C:/Users/hp/Downloads/pdf193.pdf.
3. Jonathan Weiss. 2002. Wireless Networks: Security Problems and Solutions. SANS Institute.
4. Intisar Al-Mejibli, and Sura F. Ismail. "Innovative lightweight encryption algorithm for real-time video." Journal of Intelligent and Fuzzy Systems, Vol. 36 (2019), P: 2817-2827.
5. Silex Technology Europe GmbH. 2008. The Importance of Wireless Security. White paper. SilxTchnology. http://www.silexeurope.com/media/whitepaper/importance-wireless-security_2008.pdf.
6. Tameem Hameed Obaida. Dhafar Hamed Abd. 2016. A Robust Approach for Mixed Technique of Data Encryption Between DES and RC4 Algorithm., Journal of Kufa for Mathematics and Computer Vol.3, No.2, pp 48-54.
7. W. Stalling. 2010. Cryptography and Network Security: Principles and Practices. 3rd ed. Englewood Cliffs. NJ. USA: Prentice-Hall.
8. Vernon Haberstetzer. 2005. Wireless security basics: Authentication, encryption for access points. TechTarget http://searchsecurity.techtarget.com/tip/Wireless-security-basics-Authentication-encryption-for-access-points.
9. Hossein Bidgoli. January 2006 Handbook of Information Security, Volume 1, Key Concepts, Infrastructure, Standards, and Protocols. ISBN: 978-0-471-64830-7.
10. Disha and Sukhwinder Sharma. November 2012. Comparison Of Wireless Security Protocols (WEP AND WPA2). International Journal of Computing and Corporate Research. VOLUME 2 ISSUE 6.
11. Vipin Poddar and Hitesh Choudhary. July 2014. A Comparitive Analysis of Wireless Security Protocols (WEP and WPA2). International Journal on AdHoc Networking Systems (IJANS) Vol. 4. No. 3.
12. Tagwa Ahmed Bakri Gali and Amin Babiker A/ Nabi Mustafa. 2013. A Comparative Study between WEP, WPA and WPA2 Security Algorithms. International Journal of Science and Research (IJSR). Volume 4 Issue 5.
13. BabitaDagar and Neha Goyal, February 2016. Integrating Enhanced Security Measures in WEP/WPA/WPA2-PSK. International Journal of

Innovative Research in Computer and Communication Engineering. Vol. 4. Issue 2.
14. Shikha Bansal, and Manish Mahajan. June 2017. COMPARISON OF VARIOUS WLAN SECURITIES. International Journal of Enterprise Computing and Business Systems Volume 5 Issue VI.
15. Kirti Rana, Aakanksha Jain. July 2017. Comparison and Analysis of Existing Security Protocols in Wireless Networks. International Journal for Research in Applied Science and Engineering Technology (IJRASET). Volume 5 Issue VII. Page No: ISSN : 2321-9653.
16. Samia Alblwi and Khalil Shujaee. 2017. A Survey on Wireless Security Protocol WPA2 . International Conference of Security and Management. SAM.
17. ARASH HABIBI LASHKARI and MIR MOHAMMAD SEYED DANESH. 2009. A Survey on Wireless Security protocols (WEP, WPA and WPA2/802.11i). 978-1-4244-4520-2/09/$25.00 ©IEEE.
18. Kevin Tyrrell. 2003. An Overview Of Wireless Security Issues. SANS Institute.
19. NASEER AHMAD. July 2009. Security Issues in Wireless Systems. thesis is presented as part of the Degree of Masters in Electrical Engineering with emphasis on Telecommunications. Blekinge Institute of Technology.
20. Teodor-Grigore Lupu. 2009. Main Types of Attacks in Wireless Sensor Networks. Main Types of Attacks in Wireless Sensor Networks. ISSN: 1790-5109. ISBN: 978-960-474-114-4.
21. Yulong Zou. Jia Zhu, Xianbin Wang, and Lajos Hanzo. September 2016. A Survey on Wireless Security: Technical Challenges. Recent Advances and Future Trends. Vol. 104. No. 9.
22. Shilpa Pareek, Ashutosh Gautam and Ratul Dey. April 2017. Different Type Network Security Threats and Solutions. A Review. International Journal of Computer Science (IIJCS). Volume 5. Issue 4.
23. Jason Fitzpatrick. September 21st. 2016. The Difference Between WEP, WPA, and WPA2 Wi-Fi Passwords. https://www.howtogeek.com/167783/htg-explains-the-difference-between-wep-wpa-and-wpa2-wireless-encryption-and-why-it-matters/
24. Arif Sari, Mehmet Karay. December 2015. Comparative Analysis of Wireless Security Protocols: WEP vs WPA. Int. J. Communications. Network and System Sciences.. 8. 483-491. SciRes.
25. Guillaume Lehembre. June 2005. Wi-Fi security – WEP, WPA and WPA2. http://tele1.dee.fct.unl.pt/rit2_2016_2017/files/hakin9_wifi_EN.pdf
26. Muthu Pavithran. S, Pavithran. S. August 2015. Advanced Attack Against Wireless Networks Wep, Wpa/Wpa2-Personal And Wpa/Wpa2-Enterprise. International Journal Of Scientific & Technology Research Volume 4. Issue 08. ISSN 2277-8616.
27. Nancy Owano. June 2018. WPA3 security protocol will keep Wi-Fi connections safer. Tech Xplore.
28. Jacob Kastrenakes. June 2018. Wi-Fi security is starting to get its biggest upgrade in over a decade. Circuit Breaker. https://www.theverge.com/circuitbreaker/2018/6/26/17501594/wpa3-wifi-security-certification.
29. Danilo Vezzoni. 2018. WPA3, the new wireless encryption for 2018. Belatrix Software Development Blog. 04-27-. - http://www.belatrixsf.com/blog.
30. Kowshik Bhat. August 2018. 3 Key Benefits of the WPA3 Wi-Fi Security. riverbed. https://www.riverbed.com/blogs/3-key-benefits-of-the-wpa3-wi-fi-security.html.
31. Whitson Gordon June 2018. What Is WPA3? More Secure Wi-Fi. PC. https://www.pcmag.com/article/362111/what-is-wpa3.
32. Christopher P. Kohlios and Thaier Hayajneh. September 2018. A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3". Preprints. doi: 10.20944/preprints201809.0524.v1
33. Brian Barrett. June 2018. The Next Generation of Wi-Fi Security Will Save You From Yourself. Security.